Comment

Date: November 9, 2011

RE: PS Docket No. 11–153; PS Docket No. 10–255; FCC 11–134

Federal Communications Commission (FCC)

SUMMARY

Given the relative anonymity of non-vocal communication and vulnerabilities inherent in internet protocol (IP), Next Generation 911 (NG911) may increase abuse of emergency infrastructure. In addition to the concern that abusive use of NG911 would increase administrative costs for Public Safety Answering Points (PSAPs), the FCC should weigh how these vulnerabilities threaten public safety. These factors militate against rapid implementation of a complex NG911 framework.

BACKGROUND AND ISSUE

The FCC has not considered the potential psychological and behavioral ramifications of non-vocal emergency communication. Would consumers be more likely to knowingly report erroneous emergencies through NG911 given a perception of anonymity? If so, would those reports increase administrative costs or threaten public safety?

Although the FCC raised concern over network and cyber security in this proposal's first notice of inquiry,[i] it did not make any mention of that concern in this notice of proposed rulemaking. Would IP-based NG911 increase the likelihood that a cyber-attack will block access to emergency services? If so, would those attacks increase administrative costs or threaten public safety?

ANALYSIS

Behavioral Risk

Consumers are probably more likely to abuse NG911 given a perception of anonymity using electronic communication, and such abuse poses external costs. The popularity of anonymous use of the internet is well-cataloged.[ii] Although social norms on the internet are in flux, psychologists say people deem vocal communication more revealing than text-based communication.[iii] The perception of anonymity on the internet is a catalyst to people to acting in extremely abusive ways.[iv]

It is no matter that the perception of anonymity may be unfounded from a technological standpoint since the internet service providers are usually capable of tracking IP addresses or since cellular carriers can track cell phone use, including SMS text messages. The perception alone could drive a behavioral change.

The report hopes that NG911 will decrease abusive 911 phone calls through tracking, but it fails to consider any improvement is that regard may be more than offset by NG911 abuse. Text messages

and phone apps send messages quickly and easily, but their association with casual fun could disinhibit consumers from treating NG911 seriously. Consumers, especially youths, may be inclined to experiment with NG911 in abusive ways, causing responders to chase false alarms, wasting money, and perhaps detracting from response to real crises.

Cyber Attack Risk

The internet remains vulnerable to both traditional and innovative cyber-attacks, and IP-based NG911 would suffer those same weaknesses. Denial of Service (DoS) attacks are an old fashioned but effective way to bring down internet service.[v] As technology improves, so does malicious software. The new "Conficker worm" virus is regarded as a unique new danger to government infrastructure.[vi]

The above techniques have temporarily disabled multi-million dollar companies and frustrated foreign relations between super powers. Given the severity of the potential disabling of emergency service contact, especially in a disaster, these exploitations must be guarded against despite the small chance such a disabling would occur.

CONCLUSION

The risk of abuse of NG911, given the perception of increased anonymity and IP vulnerabilities, would hurt public safety if the system were swamped with erroneous reports or disabled by cyber-attack. Increased technological security and administration is expensive. Implementation of NG911 should be slow and incremental to monitor these externalities.

---

[i] See discussion under IV(D)(6) of PS Docket No. 10-255, FCC 10-200 (Dec. 21, 2010) ("Network and Data Security Concerns").

[ii] *See, e.g.*, Elisheva F. Gross, *Adolescent Internet Use: What we expect, what teens report*, 25 Applied Developmental Psychology 633, 634-35, 644 (2004) (explaining youth use internet anonymity to experiment identity); David L. Sobel, *The Process that "John Doe" is Due: Addressing the Legal Challenge to Internet Anonymity*, 5 Va. J.L. & Tech. 3, 1522, 1524 (2000) (reviewing legal challenges to internet anonymity and citing Supreme Court opinion in *Reno v. ACLU*, 521 U.S. 844, 868 (1997), which celebrates online anonymity as a component of democracy).

[iii] *See* John Suler, *The Online Disinhibition Effect*, 7 CyberPsychology & Behavior 321 (2004) (arguing six factors cause people to act with less inhibition online, including dissociative anonymity, invisibility, and minimization of authority).

[iv] *See* Will Doig, *Homophobosphere*, The Advocate (Feb.-Mar. 2008), http://www.advocate.com/article.aspx?id=22197.

[v] *See* Reuters, *NY Times Hit by DoS Attack* (Oct. 30 2001) (explaining that DoS attack made popular New York Times website unavailable to millions for hours).

[vi] Marketplace, *The Future of Digital Warfare*, American Public Media (Nov. 4, 2011), http://marketplace.publicradio.org/display/web/2011/11/04/pm-the-future-in-digital-warfare/ (transcript and audio file).